

CLAIMS

What is claimed is:

1. A method of operating a storage device, comprising:
 - detecting data integrity errors in the storage device;
 - 5 counting each data integrity error in a count; and
 - when the count reaches a threshold limit, placing the storage device into a forced failure state.
2. The method of Claim 1, wherein the storage device is a hard disk drive.
3. The method of Claim 1, further comprising reconstructing data stored on the storage device in a restoration storage device.
4. The method of Claim 3, further comprising providing a storage device array containing said restoration storage device and said storage device.
5. The method of Claim 1, further comprising:
 - returning the storage device from the forced failure state to an operational state; and
 - setting the count to a base level.
- 20 6. The method of Claim 4, wherein said returning the storage device from the forced failure state to an operational state comprises reformatting the storage device.

7. The method of Claim 5, wherein said returning the storage device from the forced failure state to an operational state comprises decreasing the threshold limit for the storage device after placing the storage device into a forced failure state.

5 8. The method of Claim 5, wherein said returning the storage device from the forced failure state to an operational state comprises increasing the base level after placing the storage device into a forced failure state.

9. The method of Claim 1, wherein said detecting data integrity errors in the storage device 10 comprises:

retrieving data from the storage device;

comparing the retrieved data to redundancy data; and

indicating a data integrity error if the retrieved data does not correspond with the redundancy data.

45 10. The method of Claim 9, wherein said redundancy data is checksum data.

11. The method of Claim 9, wherein said retrieving data from the storage device is performed on a predetermined read schedule.

20 12. The method of Claim 11, wherein:

said retrieving data from the storage device comprises retrieving all of the data stored on the storage device; and

said comparing the retrieved data to redundancy data comprises comparing all of the data 25 stored on the storage device to redundancy data.

13. The method of Claim 1, further comprising:
tracking the time elapsed after a first data integrity error; and
decreasing the count if the time elapsed after the first data integrity error and before a
second data integrity error is greater than a preset refresh period.

5

14. The method of Claim 1, further comprising:

storing the count on the storage device.

15. A storage system, comprising:

a storage device; and

a demerit monitor coupled to the storage device for detecting data integrity errors in the
storage device, counting each data integrity error in a count, and when the count
reaches a threshold limit, placing the storage device into a forced failure state.

10

16. The storage system of Claim 15, wherein the storage device is a hard disk drive.

15

17. The storage system of Claim 15, further comprising a hard disk controller, wherein said
storage device controller includes said demerit monitor.

- 20 18. The storage system of Claim 15, further comprising an array controller, wherein said
array controller includes said demerit monitor.

19. The storage system of Claim 15, further comprising:

a storage controller coupled to a plurality of storage devices;

wherein said demerit monitor is provided in the storage controller and is coupled to each of the plurality of storage devices for detecting data integrity errors in each of the plurality of storage devices, counting each data integrity error for each of the plurality of storage devices in a count, and when the count for one of the plurality of storage devices reaches a threshold limit, placing the one storage device into a forced failure state.

20. The storage system of Claim 19, further comprising:
 - a count table maintaining the count for each of the plurality of storage devices.
 21. The storage system of Claim 15, wherein said demerit monitor returns the storage device from the forced failure state to an operational state and sets the count to a base level.
 22. The storage system of Claim 21, wherein said demerit monitor reconstructs data stored on the storage device in a restoration storage device and reformats the storage device.
 23. The storage system of Claim 21, wherein said demerit monitor decreases the threshold limit for the storage device after placing the storage device into a forced failure state.
 24. The storage system of Claim 21, wherein said demerit monitor increases the base level after placing the storage device into a forced failure state.
 25. The storage system of Claim 15, wherein said demerit monitor retrieves data from the storage device, compares the retrieved data to redundancy data, and indicates a data integrity error if the retrieved data does not correspond with the redundancy data.

26. The storage system of Claim 25, wherein the redundancy data is checksum data.
 27. The storage system of Claim 25, wherein said demerit monitor retrieves data from the storage device on a predetermined read schedule.
 28. The method of Claim 27, wherein said demerit monitor retrieves all of the data stored on the storage device, and compares all of the data stored on the storage device to redundancy data.
 29. The method of Claim 15, wherein said demerit monitor tracks the time elapsed after a first data integrity error, and decreases the count if the time elapsed after the first data integrity error and before a second data integrity error is greater than a refresh period.
 30. The method of Claim 15, wherein said count is stored on the storage device.
 31. A computer-readable medium whose contents cause a computer system to operate a storage device, by performing the steps of:
 - detecting data integrity errors in the storage device;
 - counting each data integrity error in a count; and
 - when the count reaches a threshold limit, placing the storage device into a forced failure state.
 32. The computer-readable medium of Claim 31, wherein the storage device is a hard disk drive.

33. The computer-readable medium of Claim 31, wherein the steps further comprise reconstructing data stored on the storage device in a restoration storage device.
- 5 34. The computer-readable medium of Claim 33, wherein the steps further comprise providing a storage device array containing said restoration storage device and said storage device.
- 10 35. The computer-readable medium of Claim 31, wherein the steps further comprise: returning the storage device from the forced failure state to an operational state; and setting the count to a base level.
- 15 36. The computer-readable medium of Claim 35, wherein said returning the storage device from the forced failure state to an operational state comprises reformatting the storage device.
- 20 37. The computer-readable medium of Claim 35, wherein said returning the storage device from the forced failure state to an operational state comprises decreasing the threshold limit for the storage device after placing the storage device into a forced failure state.
- 25 38. The computer-readable medium of Claim 35, wherein said returning the storage device from the forced failure state to an operational state comprises increasing the base level after placing the storage device into a forced failure state.
39. The computer-readable medium of Claim 31, wherein said detecting data integrity errors in the storage device comprises:
retrieving data from the storage device;

comparing the retrieved data to redundancy data; and
indicating a data integrity error if the retrieved data does not correspond with the
redundancy data.

5 40. The computer-readable medium of Claim 39, wherein said redundancy data is checksum
data.

41. The computer-readable medium of Claim 39, wherein said retrieving data from the
storage device is performed on a predetermined read schedule.

10

42. The computer-readable medium of Claim 41, wherein the steps further comprise:
said retrieving data from the storage device comprises retrieving all of the data stored on
the storage device; and
said comparing the retrieved data to redundancy data comprises comparing all of the data
stored on the storage device to redundancy data.

15 43. The computer-readable medium of Claim 31, wherein the steps further comprise:
tracking the time elapsed after a first data integrity error; and
decreasing the count if the time elapsed after the first data integrity error and before a
20 second data integrity error is greater than a preset refresh period.

20 44. The computer-readable medium of Claim 31, wherein the steps further comprise:
storing the count on the storage device.